Fortinet FortiManager for Microsoft Azure Quick Start Guide

FORTINET FORTIMANAGER FOR MICROSOFT AZURE QUICK START GUIDE

The following section will take you through a step-by-step process in order to deploy Fortinet FortiManager on Azure.

What is the Fortinet FortiManager for Azure?

The FortiManager family delivers the versatility you need to effectively manage your Fortinet-based security infrastructure in either a single-customer or multi-tenant environment. FortiManager drastically reduces management costs, simplifies configuration, and accelerates deployment cycles, whether you are deploying new devices, installing security policies, or distributing updates.

FortiManager also provides crucial timesaving features like device auto-discovery, group management, global policies, auditing facilities, and the ability to manage complex VPN environments. FortiManager, coupled with the FortiAnalyzer™ family of centralized logging and reporting appliances, provides a comprehensive and powerful centralized management solution for your organization.

Why FortiManager Virtual Appliance on Azure?

Placing FortiManager Virtual Appliances in the Azure cloud places these centralized management functions in close proximity to the firewalls it is managing, providing low-latency policy updates and FortiGuard Distribution Services for firewalls that do not have Internet connectivity to the FortiGuard Cloud Services.

Key Features and Benefits

1. **Integrated FortiAnalyzer Logging**—Allows for a tighter integration and correlation of events and policies. A consolidated platform allows customers to more easily deploy Fortinet management products.
2. **Hierarchical Objects Database**—Facilitates reuse of common configurations across the organization in both local and global ADOM levels.
3. **Automated Device Provisioning/Centralized Policy Configuration**—Reduces the cost of deploying new FortiGate or FortiClient installations and maintains policies across all managed assets.
4. **Role-Based Administration**—Enables distributed administration, an important requirement for larger organizations.
5. **Low-Latency FortiGuard Distribution Services**—Facilitates low-latency FortiGuard updates and web filter categorization responses.

How to Deploy the Fortinet FortiManager in Microsoft Azure Using the Azure Portal and ARM

The Fortinet FortiManager for Microsoft Azure is deployed as a virtual machine in Microsoft's Azure cloud (IaaS). You will see in the following sections how we deploy and configure the Fortinet FortiManager in the Azure Marketplace.

- Fortinet FortiManager 14-Day Trial
- Fortinet FortiManager (BYOL)—This is currently the only licensing model that is supported. Fortinet also offers a 60-day evaluation license.

BEFORE YOU GET STARTED

Before you can deploy Fortinet's FortiManager for Azure, you will need to make sure the following conditions have been met in order to successfully complete the installation:

- Create a Microsoft Azure account
- Obtain a license (choose one of the following):
    1. Purchase a Fortinet FortiManager license for Microsoft Azure http://www.windowsazure.com/en-us/account/
    2. Register to receive an evaluation license from Fortinet

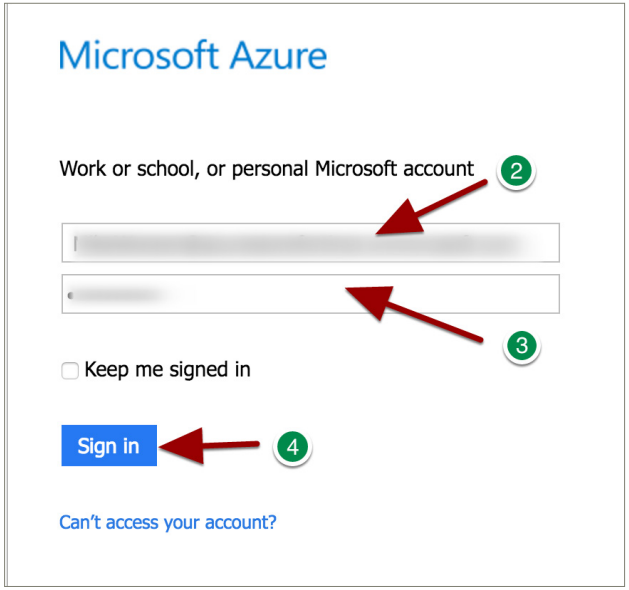
Step-by-Step Instructions to Get the Fortinet FortiManager Up and Running on Azure

The following section will take you through a step-by-step process in order to deploy Fortinet FortiManager on Azure.

1. Log In to the Azure Portal

   You access the Azure portal using the following URL: https://portal.azure.com/

2. Enter User Credentials and Sign In
   - Username: <Your Username> (2)
   - Password: <Your Password> (3)
   - Click "Sign in." (4)

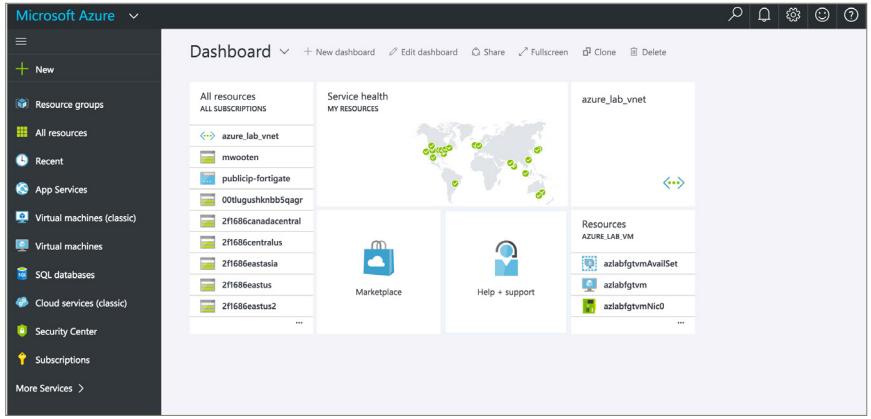


3. Successful Login to Azure

   Once you have successfully logged in to the Azure portal, you will observe the Microsoft Azure Dashboard.

   Note the following login details in the top right-hand corner of the Microsoft Azure Dashboard. If you click here, you will see options to:

   - Sign out
   - Change your password
   - View your permissions
   - View your bill

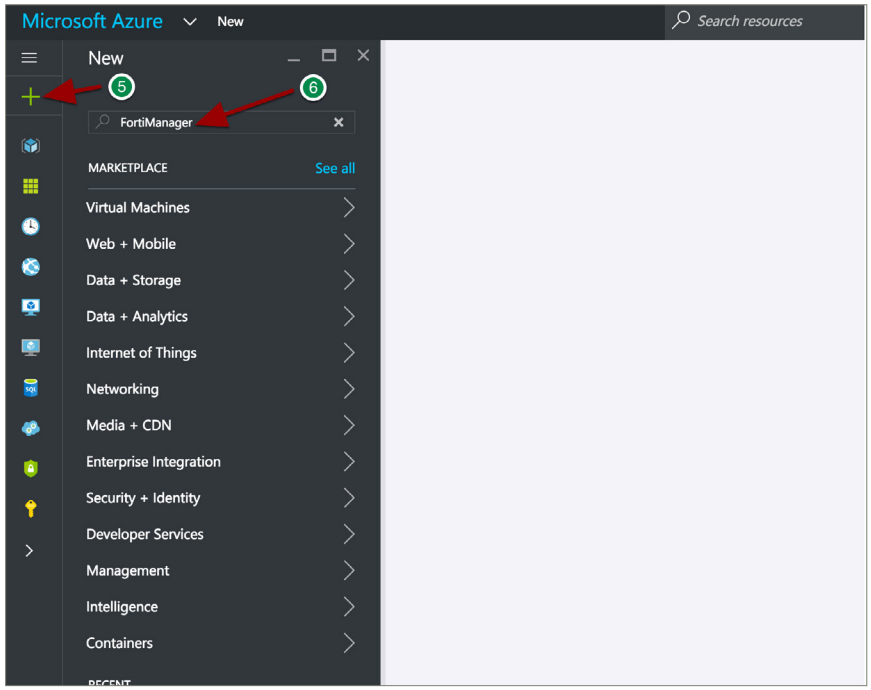


4. Creating the New Fortinet FortiManager in the Azure Marketplace

   In the Microsoft Azure portal, follow these steps:

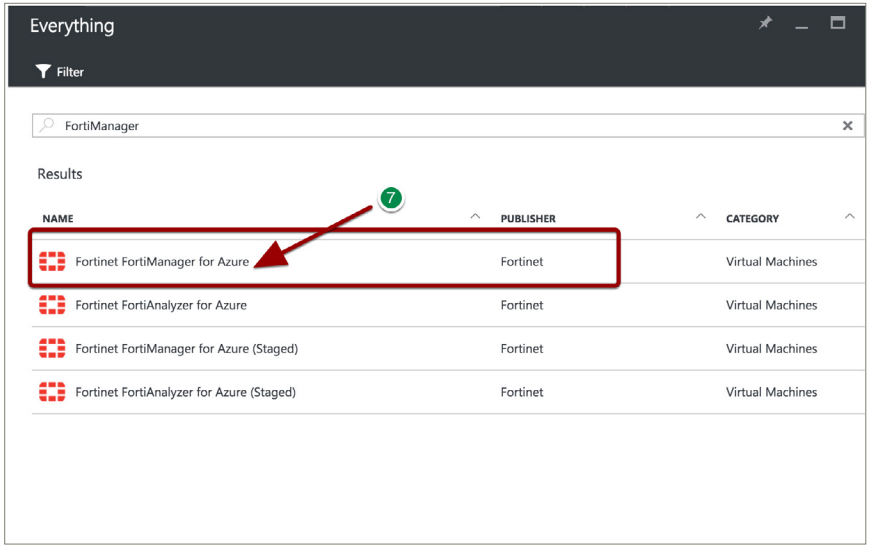
   - In the upper left-hand corner, click NEW (5).
   - In the NEW column, enter "FortiManager" in the "search the marketplace" and enter Return (6).

   NOTE: There are alternative ways of achieving the above; this is just one example.



5. FortiManager Virtual Appliances Available in the Azure Marketplace

   You will now see something similar to this, which depicts the return of the "FortiManager" search results.



6. Select the Fortinet FortiManager Deployment Model

   Once you have selected the Fortinet FortiManager VM, you will automatically be taken to the Resource Manager Panel, where you can create a deployment model.

   In the Select a deployment model, select the default Resource Manager (8).

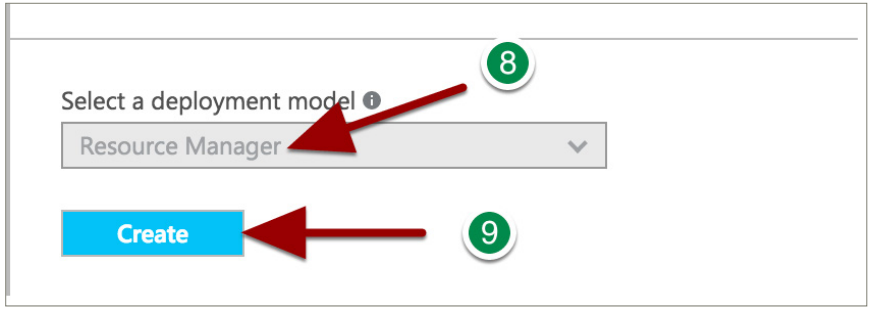
   Then click Create (9).

   NOTE: Though there is no option from the dropdown menu to select a different deployment model, this is where you would select the Classic deployment model option.

   So what exactly are the Azure deployment models?

   Azure provides two deployment models, the Classic model and the Azure Resource Manager (ARM) model. The foundation of each model is an application-programming interface (API), which is the Resource Manager API for ARM and the Service Management API for the classic model. Although developers can write software to interact with these APIs directly through the REST API, it is more common to interact with these APIs indirectly using the Azure portal, the Azure PowerShell on Windows, or the Azure Command-Line Interface (CLI) on a Windows, OS X, or Linux computer.

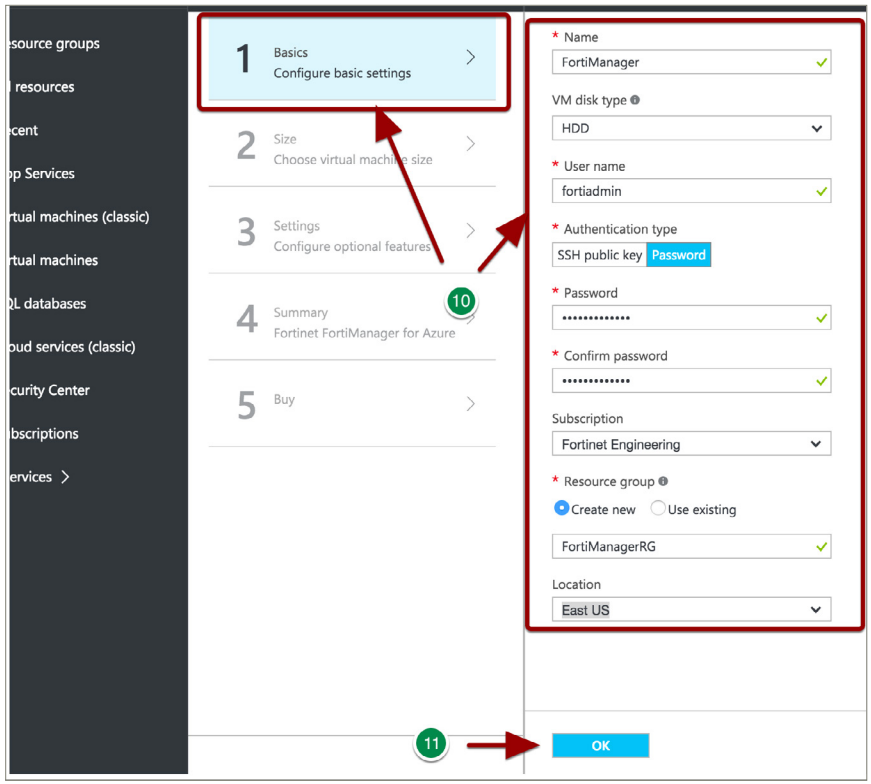
   In contrast to common belief, these two models are compatible with each other, but ARM simplifies the deployment and management of resources by managing them as a single resource group. Most newer resources support ARM, and eventually all resources will. However, how you create, configure, and manage Azure resources is different in these two models.



7. Configuring the FortiManager VM - Basic

   In the Configure basic settings panel (10), enter:

   - **FortiManager VM Name**—Enter the name of the FortiMangaer Virtual Appliance. (Only alphanumeric characters are permitted, and the value must be between 1 and 15 characters.)
   - **FortiManager Administrative Username**—Enter the administrator username for the FortiManager Virtual Appliance. (The administrator username for the FortiManager Virtual Appliance cannot be "admin.") If you do enter "admin," you will get an error message stating that the specified username is NOT allowed. In addition to this, the username can NOT contain special characters.
   - **FortiManager Password**—Enter the administrator account password for the FortiManager Virtual Appliance. (The administrator account password MUST be between 6 and 72 characters, and MUST contain characters from at least three of the following groups: uppercase characters, lowercase characters, numbers, and special characters.)
   - **Confirm password**—Re-enter the administrator account password for the FortiManager Virtual Appliance.
   - **Subscription**—The only available subscription for the FortiManager Virtual Appliance in Azure is the Pay-As-You-Go subscription model, so just leave this as "default".
   - **Resource group**—Enter the Resource group name, and note that only alphanumeric characters, periods, underscores, hyphens, and parentheses may be used. In addition to this, a Resource group name can NOT end with a "." (With Azure Resource Manager, everything you provision on Azure is a resource. You can put multiple resources into a resource group. Managing resource groups and creating and updating resource groups are the most common operations using Azure Resource Manager.)



- **Location**—Select a location from the drop-down menu. The location refers to allowing you to administer all of your Azure platform resources in a single location.

Once you have confirmed that all the above settings are correct, click "OK." (11)

NOTE: If any of the values are incorrectly defined, you will see a "Red !"; otherwise, you will see a "Green ✓."

8. Configuring the FortiManager VM - Size

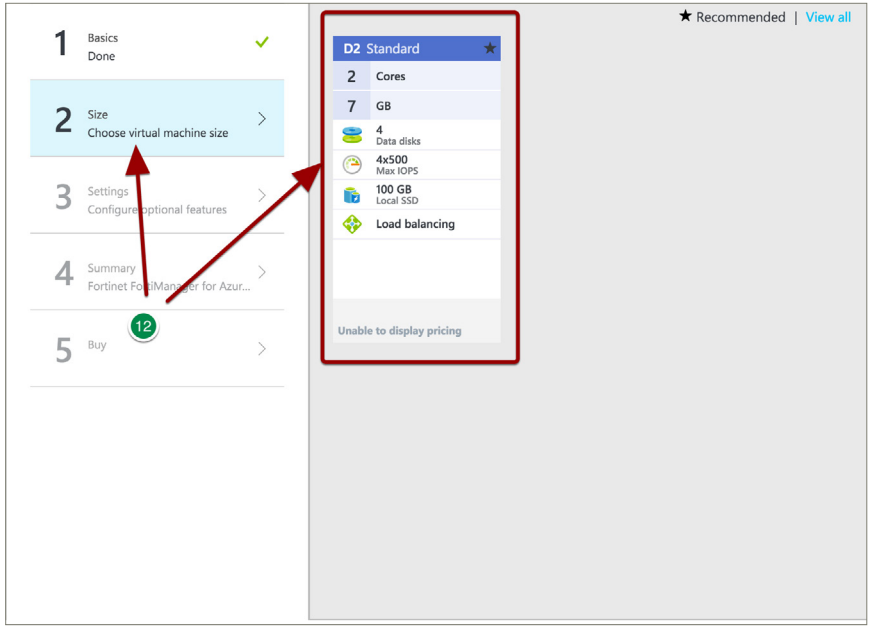
In the Azure Marketplace, the FortiManager virtual machines come in a variety of sizes, beginning with the A0 Standard up through the DS15_V2 with up to 20 cores. Each virtual machine size within each series has different limits for the amount of memory, number of NICs, maximum number of data disks, size of cache, and maximum IOPS and bandwidth.

Select the Virtual Machine Size settings (12).

The “A4 Standard” and “D4 Standard,” etc., are what are referred to as instance sizes. The instances are differentiated primarily on CPU and memory, although they also have different levels of support for multiple vNICs. For more information, please click on the following URL: https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/

When you select a “virtual machine size,” why do you not see the number of vNICs? From the “Choose virtual machine size” panel, you have no idea and would have to guess. The answer is that Azure has never prioritized multiple vNICs. So, the Azure Marketplace templates have a bias against them, and it’s extremely difficult to create a variable number of vNICs. Fortinet’s FortiManager template facilitates the creation of one vNIC.

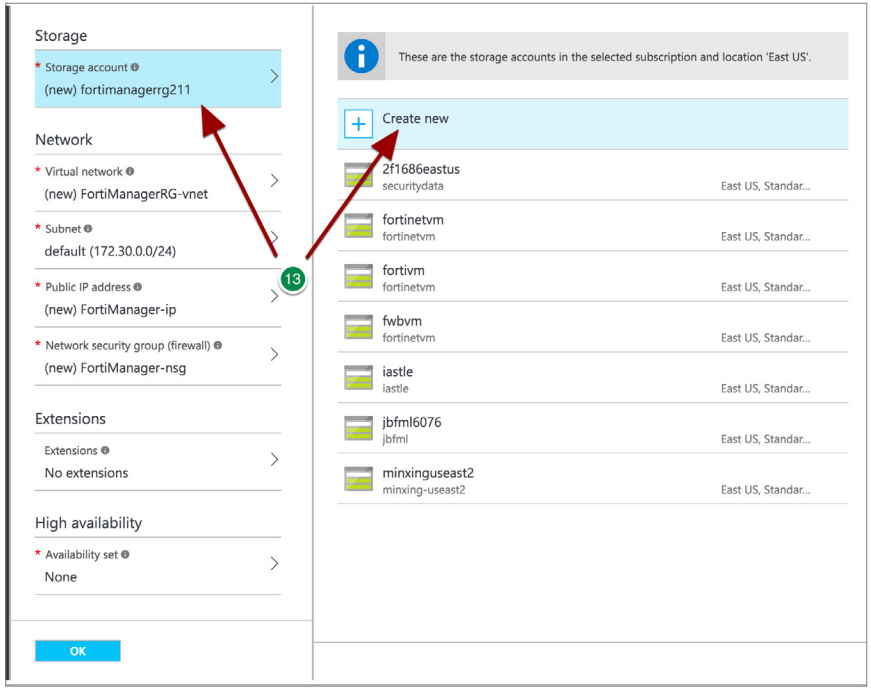
If you require more than one vNIC, you will need to deploy a custom template at this point. Please contact the Azure team (azuretech@fortinet.com) for assistance.



9. Configuring the FortiManager VM - Settings

   Storage

   Our first option for settings is Storage (13). Through the Storage workflow you can accept the default storage account associated with the newly created Resource Group, or you can select another storage account if one previously exists.



Creating a New Storage Account

If choosing one of the available storage account types is not an acceptable option, you may create a new storage account type.

Without going into the details of the different types of storage available in Azure, it is important to note (there are few exceptions) that all storage types are created from an Azure Storage Account. The Azure Storage Account in turn determines certain characteristics for the storage, such as whether the storage is locally redundant or geo-redundant, and whether the storage is based on standard HDDs or SSDs.

You can either create a new storage account or select an existing one for the FortiManager Virtual Appliance, but all resources should be in the same location (in this example: East U.S.).

Enter a Storage Account Name (14). (This account name can contain lowercase characters and numbers, and must be between 3 and 24 characters.)

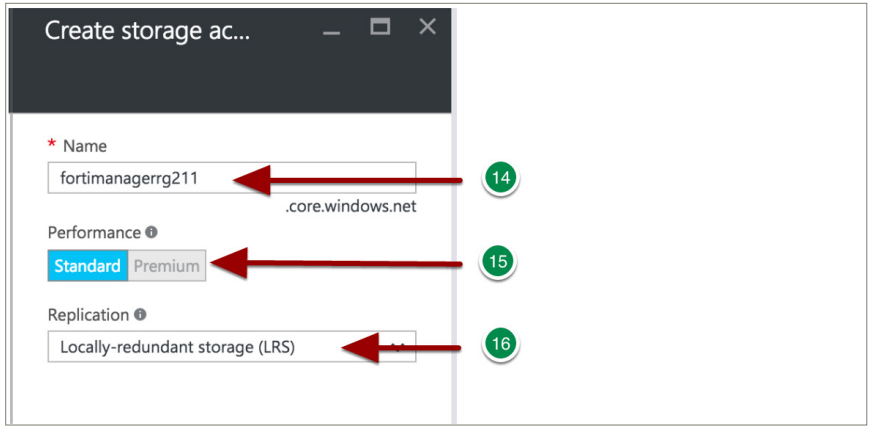
Select the Performance (15). (In this instance only standard is available.)

Select the Replication option you wish to use (16). There are two options available:

- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)

Locally redundant storage (LRS) is where all data in the Azure Storage account replicates synchronously to three different storage nodes within the primary region that was chosen when creating the Azure Storage account.

Geo-redundant storage (GRS) is where every entity is replicated into two data centers.



The data in the Azure Storage account is always replicated in order to ensure durability and high availability. Be aware that some settings cannot be changed after the storage account has been created.

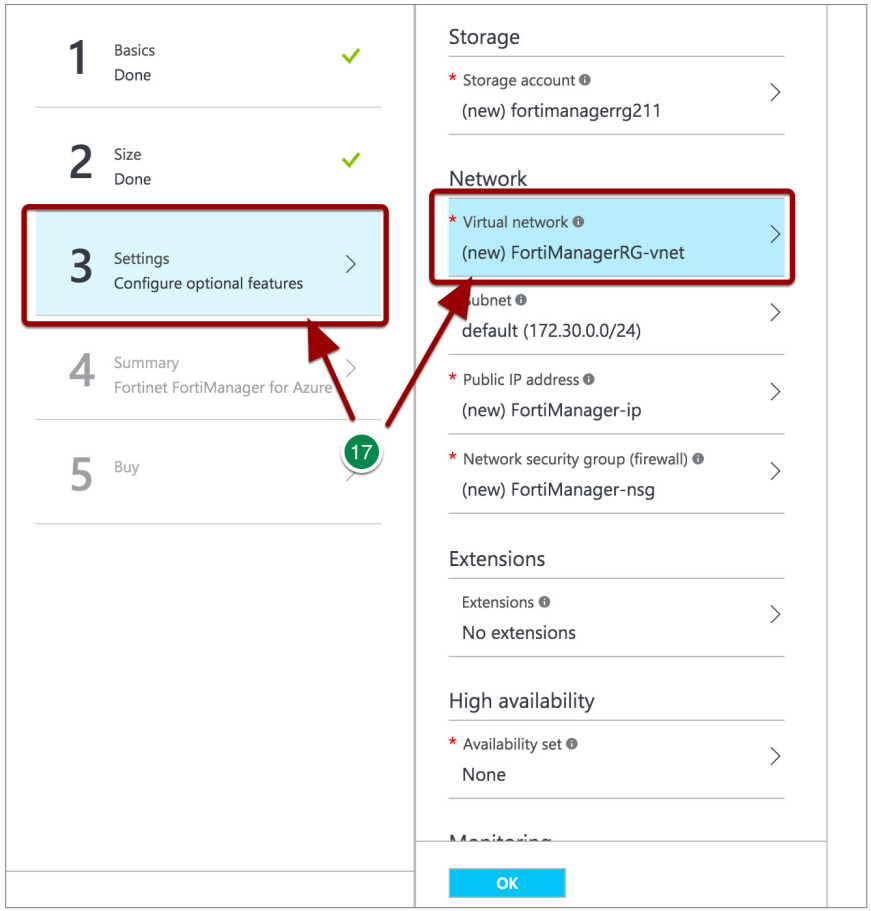
Select OK.

NOTE: No changes have been made here.

Configuring the FortiManager VM - Network

Network has several sub-tasks, which will be covered in sequence below.

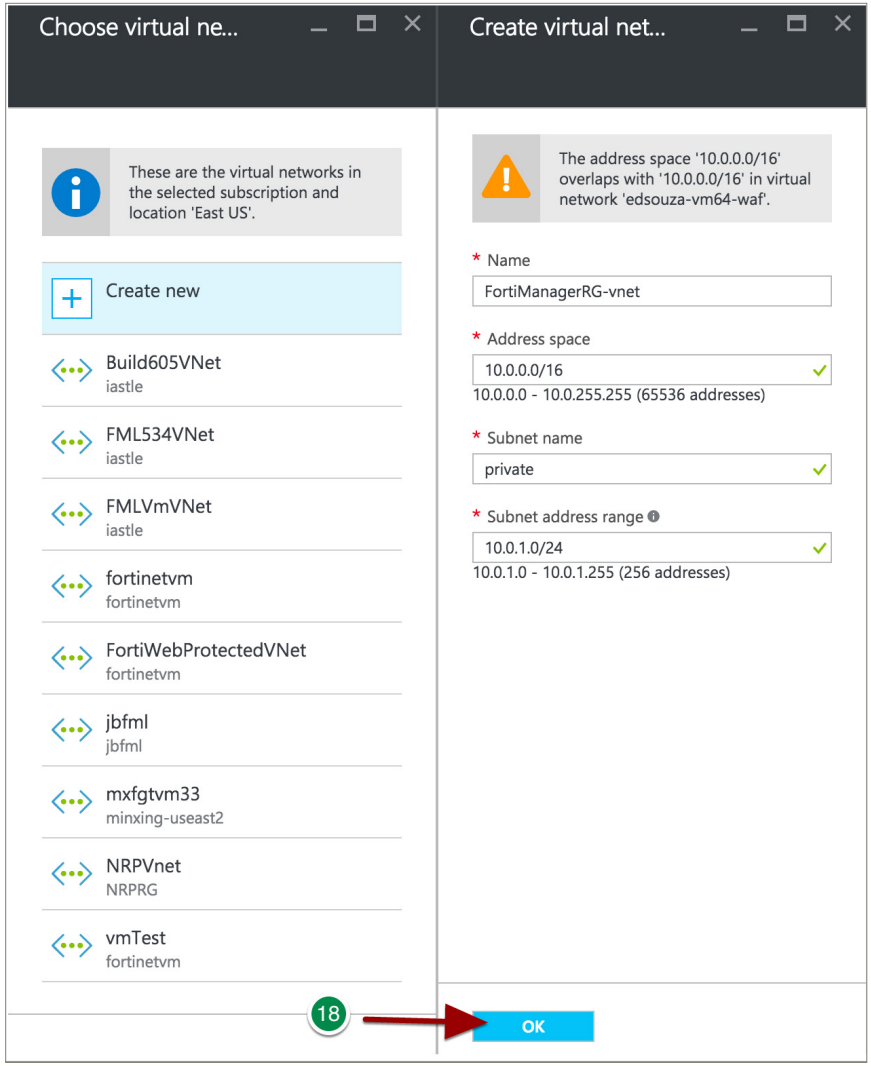
Place the FortiManager in the proper VNET and click OK (17).



Configuring the FortiManager VM - Network/Subnet

Accept the defaults for the resource group VNET or change the values to fit the deployment.

Click OK (18).



Configuring the FortiManager VM - Network/Private IP Address

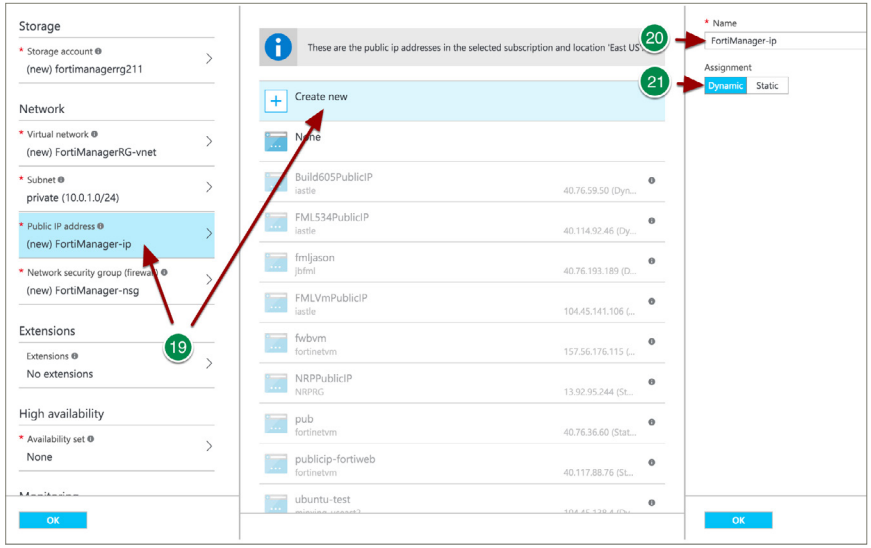
So how does the IP addressing work? When a virtual machine is deployed into a virtual network (VNET), its internal IP address is assigned from the subnet you specify and is dependent on the order in which it was provisioned, unless a static IP has been specified. For example, the FortiManager private subnet created uses the address prefix of 10.0.1.0/24. The first four IP addresses of each subnet are reserved. With this knowledge in hand, it is easy to deduce that the first IP address available in this subnet will be 10.0.1.5 Unless otherwise specified, a virtual machine will be assigned the next available IP address from the subnet to which it was assigned at provisioning time.

In this example, we want the FortiManager to be provided a static IP address of 10.0.1.253 on the private subnet side, so we can configure the FortiGate to NAT the public IP address assigned to the FortiManager to the IP address statically assigned on the private side.

Choose “Public IP address” on the left menu and “Create new” on the center menu (19).

Now provide a name for the IP address resource (20).

Choose “Dynamic” for the assignment (21).



Configuring the FortiManager VM - Network/Network Security Group (Firewall)

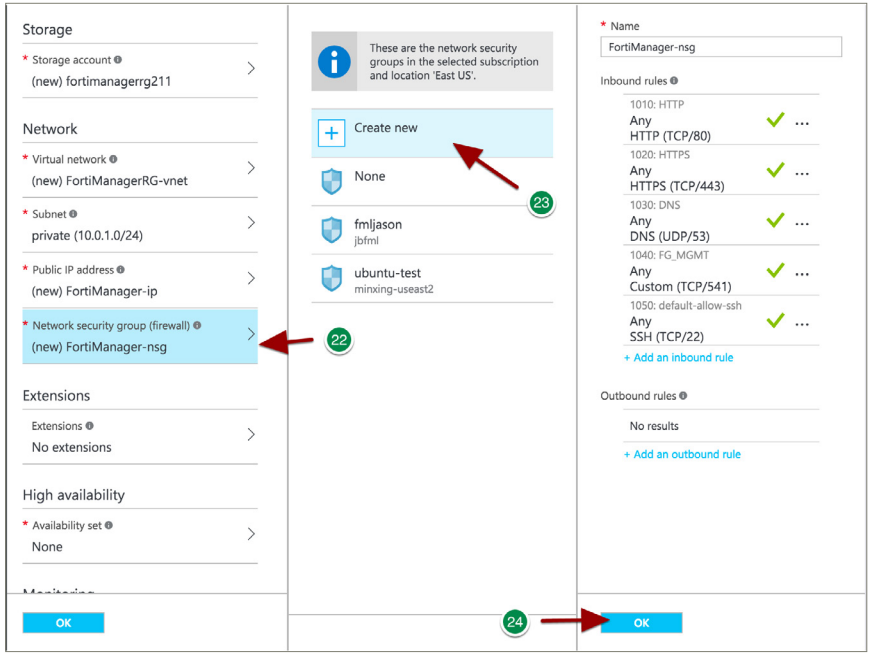
Again we will leave the default Network security group; however, these are the predefined services allowed to the VM. Here you can Add an inbound rule or select custom security groups already defined.

Choose “Network security group” on the left menu (22).

Choose “Create new” on the center menu (23).

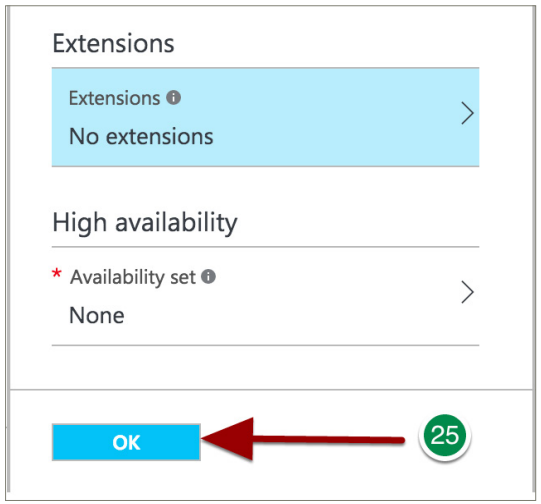
Accept the defaults on the right menu and click “OK” (24).

NOTE: No changes have been made here.



Configuring the FortiManager VM - Extensions/High Availability

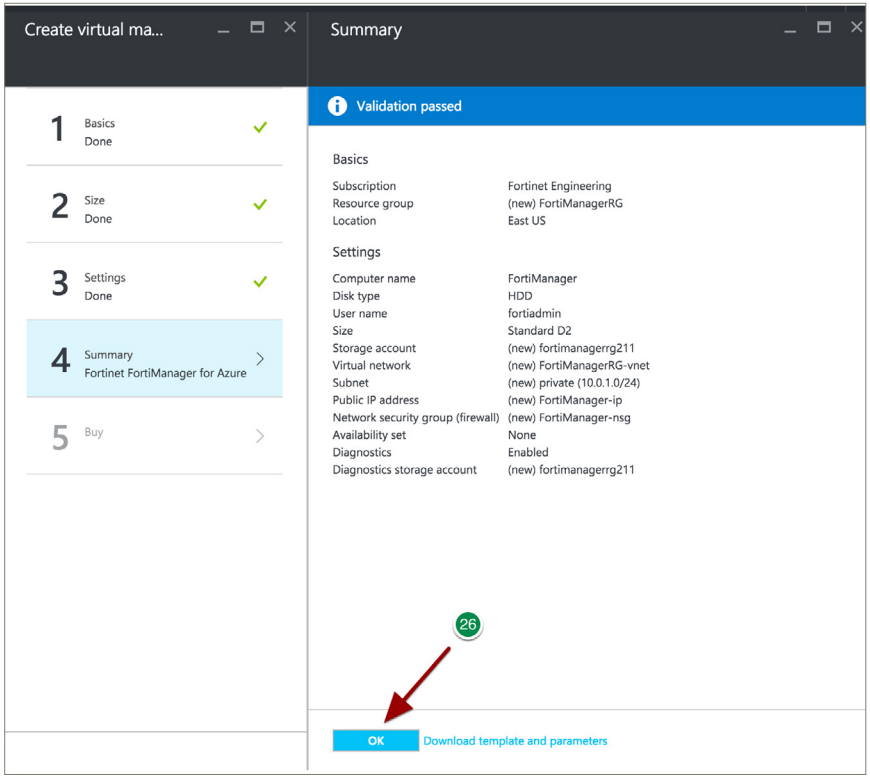
For purposes of this guide and deployment model, we will leave the defaults for Extensions/High availability/Monitoring (25).



10. Configuring the FortiManager VM - Summary

    After selecting “OK,” a validation process will take place and your configuration will be validated. If successful, you will see Validation passed.

    Select OK (26).



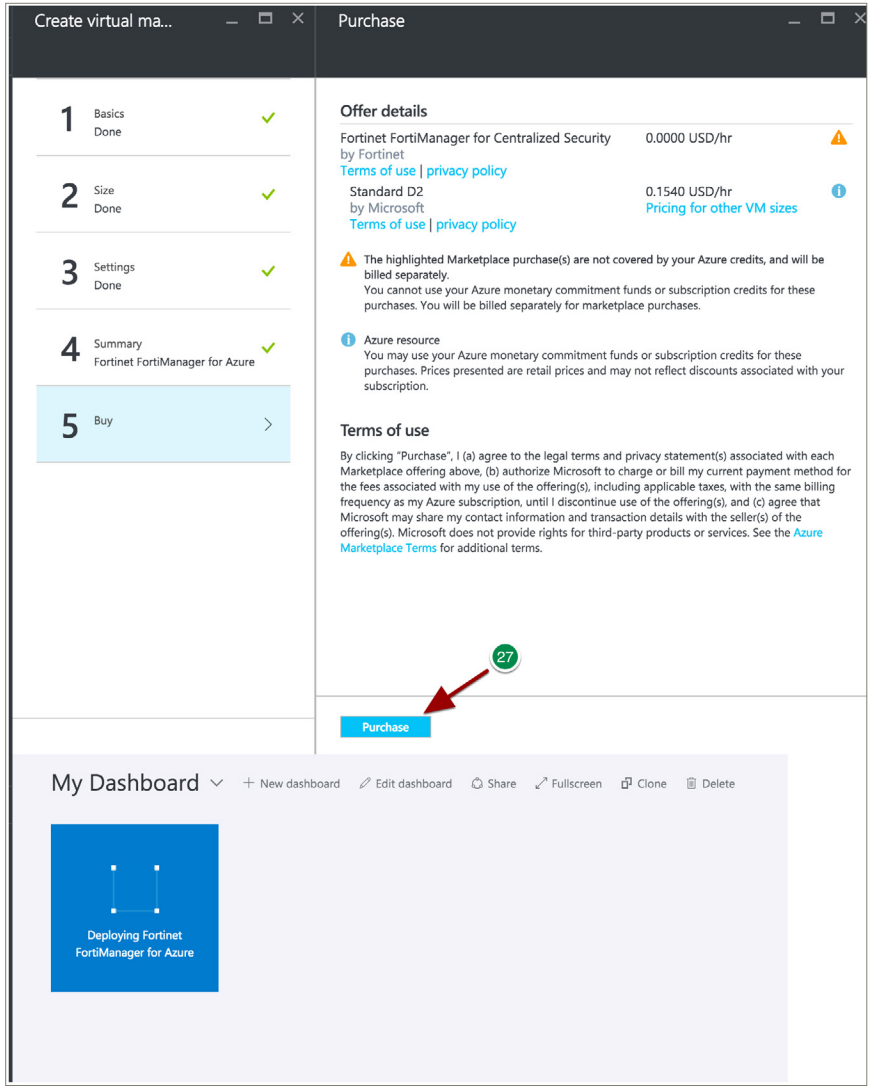
11. Configuring the FortiManager VM - Buy

After the Fortinet FortiManager VM Configuration has been completed, you now are required to select purchase.

Select Purchase (27).

NOTE: Purchase just means that you are going to be paying Azure for the virtual machine use time. You still must obtain a license separately from Fortinet, Inc.

After selecting “Purchase,” you should see the “Deploying FortiManager” screen while Azure allocates the resources for the VM.

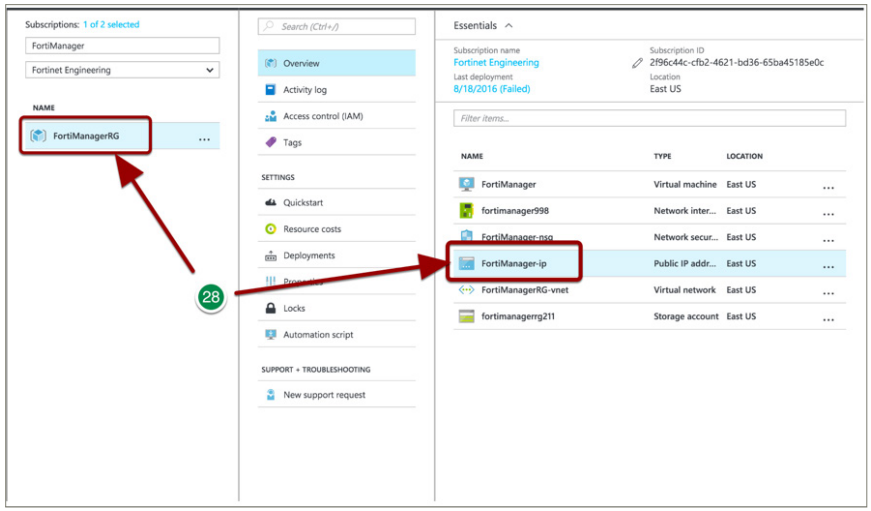


12. Connect to the FortiManager Azure VM by Public IP

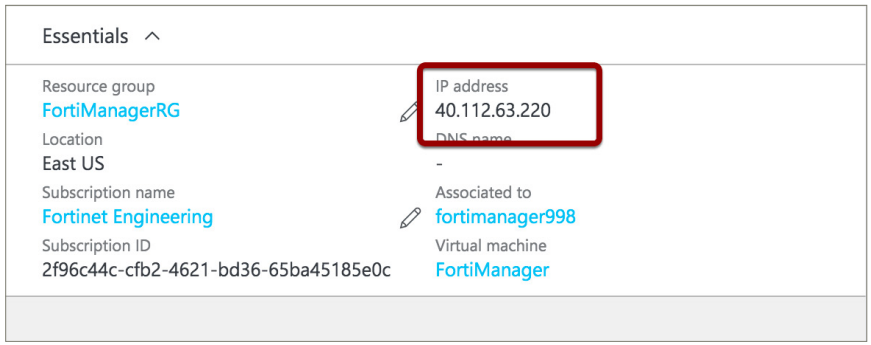
    In order to be able to connect to the FortiManager Public IP Address, we need to know what this IP address is.

    To accomplish this:

    Once again from the FortiManagerRG Resource Group, select FortiManager-ip (28).



    This will expose the Public IP Address, which is: 40.112.63.220.



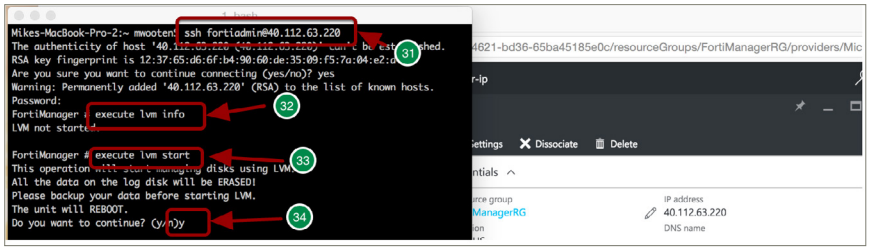
Connect to the FortiAnalyzer Azure VM by Public IP via SSH and Start LVM

SSH to our found Public IP Address (29), which is: 40.112.63.220.

Recall in Step 10 we defined both the username and password, which are as follows and are required to connect to the FortiManager Virtual Appliance UI:

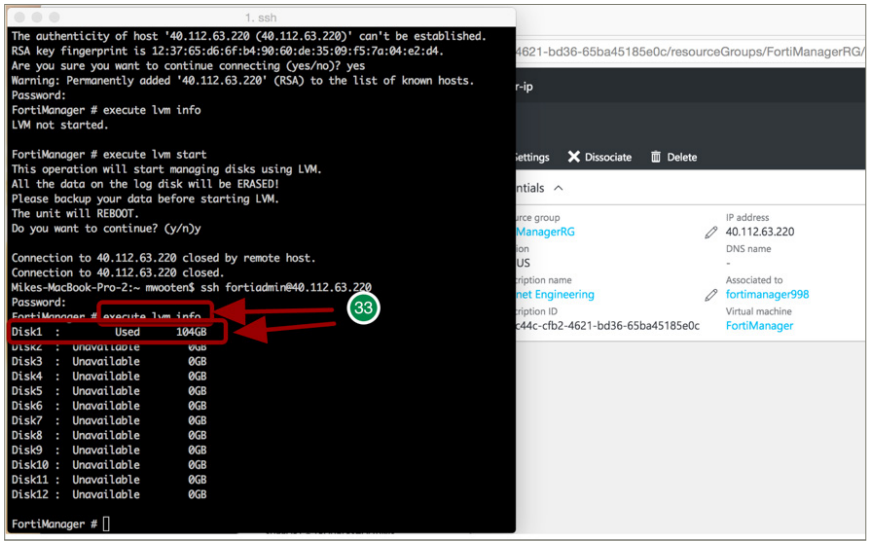
- FortiAnalyzer Administrative Username: fortiadmin
- FortiAnalyzer Password: <the password you entered>
- Type execute lvm info (30).
- Type execute lvm start (31).
- Type y (32).

FortiManager VM will reboot and SSH connectivity will go red.



Ensure you regain connectivity to the FortiManager VM after starting the LVM service. This could take a couple of minutes.

Type execute lvm info and verify LVM service is started and the newly created disk is attached (33).

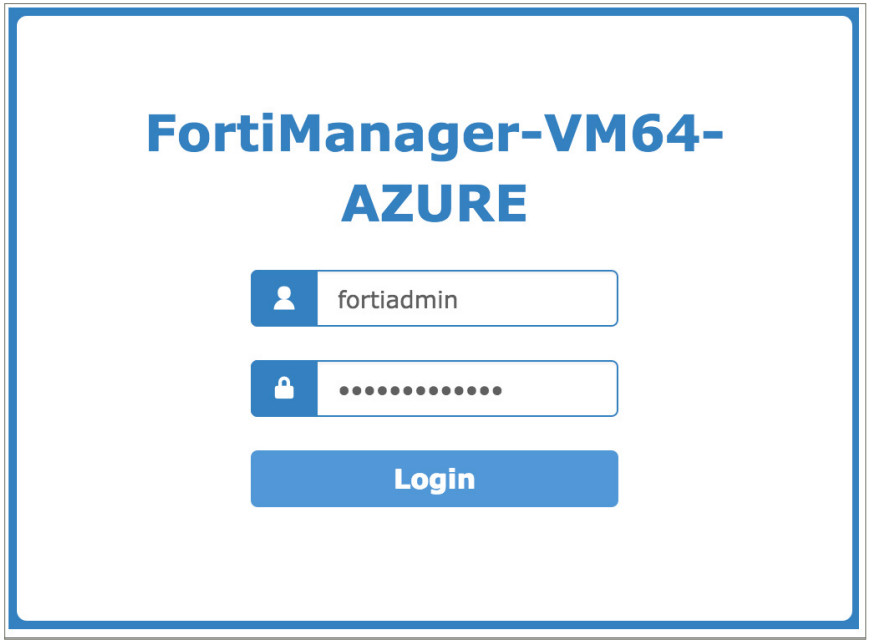


Connect to the FortiManager Azure VM by Public IP via HTTPS

HTTPS to our found Public IP Address, which is: 40.112.63.220.

Recall in Step 10 we defined both the username and password, which are as follows and are required to connect to the FortiManager Virtual Appliance UI:

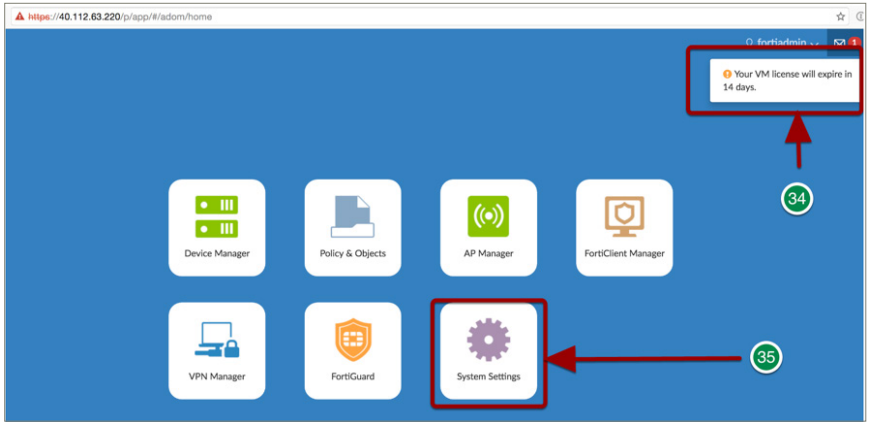
- FortiAnalyzer Administrative Username: fortiadmin
- FortiAnalyzer Password: <the password you entered>



13. Verify Temporary License - Check Messages

    Click on your messages (34). You will see Your VM license will expire in 14 days.

    Click on System Settings (35).

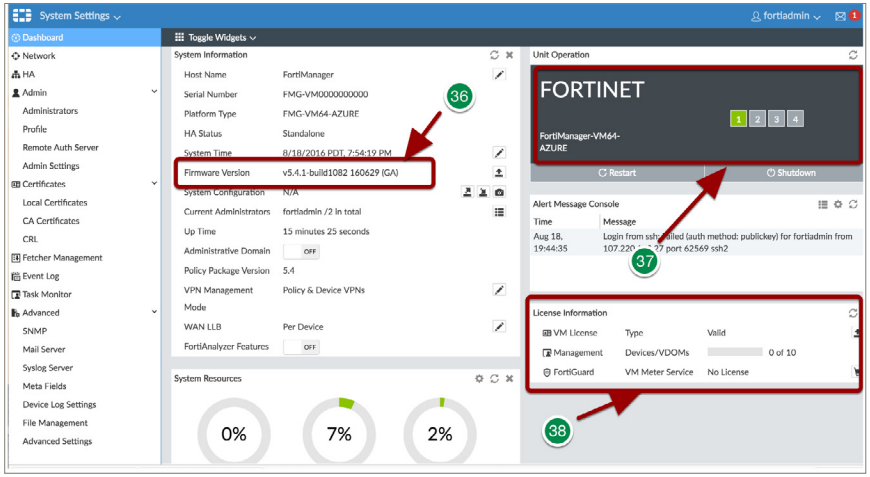


14. Verify Unit Operations - Firmware Version/Connectivity/License Information

    Firmware Version (36).

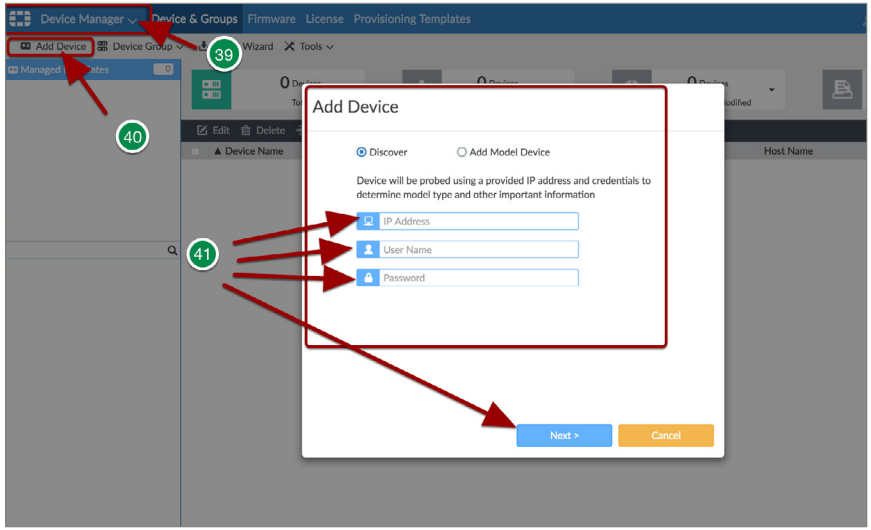
    Connectivity (37).

    License Information (38). This is also where you would upload your BYOL obtained from Fortinet Inc.



Add Your First Device to Your FortiManager

- Switch to the Device Manager tab (39).
- Click Add Device (40).
- Provide the IP address, user name, and password and import your first device into FortiManager (41).



Support

For more in-depth instructions, please refer to http://docs.fortinet.com/ for administration guides or email your support questions to azuretech@fortinet.com.

v1.0 09.07.16